

CLAIMS

1. A system for analyzing network traffic comprising:
 - a plurality of subscriber units and a default router default router interconnected by a network, said network operable to direct routed traffic to an appropriate subscriber unit and further operable to direct unrouted traffic to said default router default route generator; and
 - an analyzer connected to said default router default router for determining patterns of activity within said unrouted traffic.
2. The system according to claim 1 wherein said activity is selected from the group consisting of worms, viruses, Trojan horses, scanners.
3. The system according to claim 1 wherein said activity is a misconfiguration of a network routing table in a second network adjacent to said network.
4. The system according to claim 3 wherein said misconfiguration is a result of said second network routing traffic to a third network adjacent said network via said network.
- 15 5. The system according to claim 3 wherein said misconfiguration is a breach of a service contract between an operator of said network and an operator of said second network.
6. The system according to claim 5 further comprising a means for assessing a penalty against an operator of said second network, said penalty corresponding to said breach of contract.
- 20 7. The system according to claim 1 wherein at least one of said patterns is plurality of attempts by one of said subscriber units to send unrouted traffic.
8. The system according to claim 7 wherein said attempts occur at substantially identical intervals of time.

9. The system according to claim 1 wherein at least one of said patterns includes a subscriber unit originating unrouted traffic from at least one predefined port and attempting to send traffic to another at least one predefined port.
10. The system according to claim 1 wherein at least one of said patterns includes a subscriber unit originating traffic of a first type of protocol.
5
11. The system according to claim 1 further comprising a honey pot connected to said analyzer for responding to said unrouted traffic.
12. The system according to claim 11 wherein said honey pot is operable to permit itself to be infected with a malicious code associated with said unrouted traffic.
- 10 13. The system according to claim 12 wherein said honey pot includes a malicious code scanner for identifying said malicious code once said honey pot computer is infected.
14. The system according to claim 1 further comprising a means for isolating one of said subscriber units from said network if said analyzer determines a pattern of activity associated therewith is malicious.
- 15 15. The system according to claim 1 further comprising a means for notifying one of said subscriber units if said analyzer determines a pattern of activity associated therewith is malicious.
16. The system according to claim 15 further comprising a means for charging a fee to a subscriber associated with said one of said subscriber units.
- 20 17. The system according to claim 1 further comprising a means for providing said analyzer with updated definitions of known patterns of malicious traffic.
18. A traffic analyzer comprising:

an interface for connecting to a network, said network operable to interconnect a plurality of subscriber units, said network further operable to direct routed traffic to an appropriate subscriber unit and further operable to direct unrouted traffic to said interface; and,
25

a processing means connected to said interface, said processing means operable to determine patterns of activity within said unrouted traffic.

19. The analyzer according to claim 18 wherein said activity is selected from the group consisting of worms, viruses, Trojan horses, scanners.

5 20. The analyzer according to claim 18 wherein said activity is a misconfiguration of a network routing table in a second network adjacent to said network.

21. The analyzer according to claim 20 wherein said misconfiguration is a result of said second network routing traffic to a third network adjacent to said network via said network.

10 22. The analyzer according to claim 20 wherein said misconfiguration is a breach of a service contract between an operator of said network and an operator of said second network.

23. The analyzer according to claim 18 wherein at least one of said patterns is plurality of attempts by one of said subscriber units to send unrouted traffic.

24. The analyzer according to claim 23 wherein said attempts occur at substantially identical intervals of time.

15 25. The analyzer according to claim 18 wherein at least one of said patterns includes a subscriber unit originating unrouted traffic from at least one predefined port and attempting to send traffic to another at least one predefined port.

26. The analyzer according to claim 18 wherein at least one of said patterns includes a subscriber unit originating traffic of a first type of protocol.

20 27. The analyzer according to claim 18 further comprising a honey pot connected to interface analyzer for responding to said unrouted traffic.

28. The analyzer according to claim 27 wherein said honey pot is operable to permit itself to be infected with a malicious code associated with said unrouted traffic.

29. The analyzer according to claim 28 wherein said honey pot includes a malicious code scanner for identifying said malicious code once said honey pot computer is infected.

30. The analyzer according to claim 18 further comprising a means for instructing said to network isolate one of said subscriber units from said network if said analyzer determines a pattern of activity associated therewith is malicious.

5 31. The analyzer according to claim 18 further comprising a means for notifying one of said subscriber units if said processing means determines a pattern of activity associated therewith is malicious.

10 32. The analyzer according to claim 18 further comprising a means for providing said analyzer with updated definitions of known patterns of malicious traffic.

15 33. The analyzer according to claim 18 wherein said interface is a default router operable to instruct a routing table associated with said network to deliver unrouted traffic to said default route generator.

20 34. A default router for connecting to a network that interconnects a plurality of subscriber units; said network operable to direct routed traffic in said network to an appropriate subscriber unit; said default router operable to instruct said network to direct unrouted traffic to said default route generator.

25 35. The default router of claim 34 wherein said network further includes a routing table and wherein said default router instructs said network to direct unrouted traffic by creating an entry in said routing table associated with said default route generator.

30 36. A network routing table for use in association with a network that interconnects a plurality of subscriber units; said network operable to access said network routing table to direct routed traffic in said network to an appropriate subscriber unit; said network further operable to access said network routing table to direct unrouted traffic in said network to a traffic analyzer.

35 37. A method of analyzing traffic in a network comprising the steps of:
receiving traffic from at least one of a plurality of subscriber units interconnected by said network;

delivering said traffic to a destination subscriber unit if said traffic is routed;

analyzing said traffic for patterns of activity in said traffic if said traffic is unrouted.

38. The method according to claim 37 wherein said activity is selected from the group consisting of worms, viruses, Trojan horses, scanners.

5 39. The method according to claim 37 wherein said activity is a misconfiguration of a network routing table in a second network adjacent to said network.

40. The method according to claim 39 wherein said misconfiguration is a result of said second network routing traffic to a third network adjacent to said network via said network.

10 41. The method according to claim 39 wherein said misconfiguration is a breach of a service contract between an operator of said network and an operator of said second network.

42. The method according to claim 41 further comprising the step of assessing a penalty against an operator of said second network, said penalty corresponding to said breach of contract.

15 43. The method according to claim 37 wherein at least one of said patterns is plurality of attempts by one of said subscriber units to send unrouted traffic.

44. The method according to claim 43 wherein said attempts occur at substantially identical intervals of time.

20 45. The method according to claim 37 wherein at least one of said patterns includes a subscriber unit originating unrouted traffic from at least one predefined port and attempting to send traffic to another at least one predefined port.

46. The method according to claim 37 wherein at least one of said patterns includes a subscriber unit originating traffic of a first type of protocol.

47. The method according to claim 37 further comprising the step of responding to said unrouted traffic.

48. The method according to claim 47 further comprising the step of permitting an infection in a honey pot computer of a malicious code in associated with said unrouted traffic.
49. The method according to claim 48 further comprising the step of, after said permitting step, scanning said honeypot computer to identify said malicious code once.
- 5 50. The method according to claim 37 further comprising the step of isolating one of said subscriber units from said network if said pattern of activity associated with said one of said subscriber units is determined to be malicious.
51. The method according to claim 37 further comprising the step of notifying one of said subscriber units if said pattern of activity associated with said one of said subscriber units is determined to be malicious.
- 10 52. The method according to claim 51 further comprising the step of charging a fee to a subscriber associated with said one of said subscriber units.
53. The method according to claim 37 further comprising the step of providing updated definitions of known patterns of malicious traffic.
- 15 54. The method according to claim 37 further comprising the step of notifying one of said subscriber units if said pattern of activity associated with said one of said subscriber units is determined to be malicious, said notifying including offering a software tool for removing code from said at least one subscriber unit that is responsible for generating such malicious activity.
- 20 55. A system comprising:
 - means for receiving network traffic from at least one subscriber unit coupled to a network; and
 - means for detecting an infection problem on said subscriber unit with use of said received network traffic.

56. A system according to claim 55, further comprising means for offering to a person associated with the subscriber unit, an application to at least one of protect and destroy the infection problem if an infection problem is detected on the subscriber unit.

57. A system for analyzing network traffic comprising:

5 a network;

a plurality of subscriber units connected to said network;

a default router connected to said network;

a network router for directing traffic that is:

addressed to one of said subscriber units to a corresponding said subscriber unit; and

10 unaddressed to any said subscriber unit to said default route generator;

an analyzer connected to said default router for determining patterns of activity within traffic directed to said default route generator.

58. A method of analyzing traffic comprising the steps of:

15 receiving unrouted network traffic originating from at least one of a plurality of subscriber units; and,

analyzing said traffic for patterns of activity in said traffic.